02.02.01

JP 01/772

EO

#4

日本国特許庁
PATENT OFFICE JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　８月　７日

出願番号
Application Number: 特願２０００－２３８０７７

出願人
Applicant (s): ソニー株式会社

09/937797

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００１年　３月　２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３０１５１６７

【書類名】　特許願

【整理番号】　0000460905

【提出日】　平成12年 8月 7日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/30

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　橋本　主税

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　佐竹　清

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　金巻　裕史

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　齋藤　真

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100094053

【弁理士】

【氏名又は名称】　佐藤　隆久

【手数料の表示】

【予納台帳番号】　014890

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707389

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報記録方法、情報復元方法およびそれらの装置と記録媒体

【特許請求の範囲】

【請求項１】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割し、

前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する

情報記録方法。

【請求項２】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項１に記載の情報記録方法。

【請求項３】

前記所定の情報を暗号化し、

当該暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する

請求項１に記載の情報記録方法。

【請求項４】

前記複数のモジュールをそれぞれ暗号化し、

当該暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する

請求項１に記載の情報記録方法。

【請求項５】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出し、

当該読み出したモジュールを合成して前記所定の情報を復元する

情報復元方法。

【請求項６】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項５に記載の情報復元方法。

【請求項７】

前記読み出したモジュールを合成した後に復号して前記所定の情報を復元する

請求項５に記載の情報復元方法。

【請求項８】

前記読み出したモジュールを復号した後に合成して前記所定の情報を復元する

請求項５に記載の情報復元方法。

【請求項９】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割する情報分割手段と、

前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む書き込み手段と

を有する情報記録装置。

【請求項１０】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項９に記載の情報記録装置。

【請求項１１】

前記所定の情報を暗号化する暗号化手段

をさらに有し、

前記情報分割手段は、

前記暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する

請求項９に記載の情報記録装置。

【請求項１２】

前記複数のモジュールをそれぞれ暗号化する暗号化手段

をさらに有し、

前記書き込み手段は、

前記暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む

請求項９に記載の情報記録装置。

【請求項１３】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出す読み出し手段と、

当該読み出したモジュールを合成して前記所定の情報を復元する情報合成手段と

を有する情報復元装置。

【請求項１４】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項１３に記載の情報復元装置。

【請求項１５】

前記合成して得た情報を復号する復号手段

をさらに有する

請求項１３に記載の情報復元装置。

【請求項１６】

前記読み出したモジュールを復号する復号手段

をさらに有し、

前記情報合成手段は、前記復号したモジュールを合成して前記所定の情報を復元する

請求項１３に記載の情報復元装置。

【請求項１７】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割した場合に、前記複数のモジュールのうち一のモジュールが記録された

記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、記録媒体に保持される情報の秘匿性を高めることができる情報記録方法、情報復元方法およびそれらの装置に関する。

【０００２】

【従来の技術】

近年、電子商取り引きの発達に伴い、ユーザの個人ＩＤ情報や暗証番号、取り引きの履歴情報、ユーザの名前、住所、経歴および職業などの個人情報などの秘匿性のある情報を、サーバ装置や端末装置などが管理する場合が多くなっている。

【０００３】

サーバ装置や端末装置では、例えば、特開平１１－２７２６７８１号公報に示されるように、上述したような秘匿性のある情報を、所定の暗号鍵で暗号化して、コンピュータに内蔵されたＨＤＤ(Hard Disk Drive) や、携帯性のあるＣＤ－ＲＯＭ、フロッピーディスク、ＰＣカードなどの記録媒体に記録している。

【０００４】

【発明が解決しようとする課題】

しかしながら、上述した従来のサーバ装置や端末装置では、通常、秘匿性のある情報を単体の記録媒体に記録しており、その記録媒体が盗まれたり、不正にコピーされると、当該情報の秘匿性が失われてしまうという問題がある。

このような秘匿性のある情報は、通常、暗号化されて記録媒体に記録されるが、暗号化は復号（解読）される可能性があり、秘匿性を保持する上で十分ではない。

【０００５】

本発明は上述した従来技術の問題点に鑑みてなされ、情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録方法、情報復元方法およびそれらの装置と記録媒体に関する。

【０００６】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第１の発明の情報記録方法は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割し、前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する。

【０００７】

また、第１の発明の情報記録方法は、好ましくは、前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である。

【０００８】

また、第１の発明の情報記録方法は、好ましくは、前記所定の情報を暗号化し、当該暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する。

【０００９】

また、第１の発明の情報記録方法は、好ましくは、前記複数のモジュールをそれぞれ暗号化し、当該暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する。

【００１０】

また、第２の発明の情報復元方法は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出し、当該読み出したモジュールを合成して前記所定の情報を復元する。

【００１１】

また、第２の発明の情報復元方法は、好ましくは、前記複数のモジュールが記

録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である。

【００１２】

また、第２の発明の情報復元方法は、好ましくは、前記読み出したモジュールを合成した後に復号して前記所定の情報を復元する。

【００１３】

また、第２の発明の情報復元方法は、好ましくは、前記読み出したモジュールを復号した後に合成して前記所定の情報を復元する。

【００１４】

また、第３の発明の情報記録装置は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割する情報分割手段と、前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む書き込み手段とを有する。

【００１５】

また、第４の発明の情報復元装置は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出す読み出し手段と当該読み出したモジュールを合成して前記所定の情報を復元する情報合成手段とを有する。

【００１６】

また、第５の発明の記録媒体は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割した場合に、前記複数のモジュールのうち一のモジュールが記録されている。

【００１７】

【発明の実施の形態】

以下、本発明の実施形態に係わる情報記録装置および情報復元装置について説明する。

<u>第１実施形態</u>

図１は、本実施形態の情報記録装置１の構成図である。

図１に示すように、情報記録装置１は、読み出し回路１０、暗号化回路１１、情報分割回路１２、書き込み回路１３，１４を有する。

情報記録装置１は、記録媒体１５から読み出した個人情報Ｄ１を暗号化した後に、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ３，Ｄ４に分割し、モジュールＤ３を記録媒体１６に書き込み、モジュールＤ４を記録媒体１７に書き込む。

本実施形態において、記録媒体１５，１６，１７は、ＨＤＤ装置や、携帯性のあるＣＤ－ＲＯＭ、フロッピーディスク、ＰＣカードなどの記録媒体である。

【００１８】

読み出し回路１０は、記録媒体１５から読み出した個人情報Ｄ１を暗号化回路１１に出力する。

個人情報Ｄ１は、図２に示すように、情報Ｄａｔａ１～ＤａｔａＮからなる。

また、個人情報Ｄ１は、例えば、ユーザの個人ＩＤ情報や暗証番号、取り引きの履歴情報、ユーザの名前、住所、経歴および職業などの秘匿性のある情報である。

【００１９】

暗号化回路１１は、所定の暗号鍵を用いて、読み出し回路１０から入力した個人情報Ｄ１を暗号化して個人情報Ｄ２を生成し、これを情報分割回路１２に出力する。

暗号化された個人情報Ｄ２は、図２に示すように、それぞれ情報Ｄａｔａ１～ＤａｔａＮを暗号化した情報Ｄａｔａ１’～ＤａｔａＮ’からなる。

【００２０】

情報分割回路１２は、暗号化回路１１から入力した暗号化された個人情報Ｄ２を、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ３，Ｄ４に分割し、モジュールＤ３を書き込み回路１３に出力し、モジュールＤ４を書き込み回路１４に出力する。

図２に示すように、情報分割回路１２は、情報Ｄ２内の情報Ｄａｔａ１’～ＤａｔａＮ’を、それぞれ情報Ｄａｔａ１Ａ’およびＤａｔａ１Ｂ’、情報Ｄａｔ

ａ２Ａ’およびＤａｔａ２Ｂ’、情報Ｄａｔａ３Ａ’およびＤａｔａ３Ｂ’、．．．．、情報ＤａｔａＫＡ’およびＤａｔａＫＢ’、．．．．．、情報ＤａｔａＮＡ’およびＤａｔａＮＢ’に分割する。

そして、情報分割回路１２は、情報Ｄａｔａ１Ａ’，Ｄａｔａ２Ａ’，Ｄａｔａ３Ａ’，．．．，ＤａｔａＫＡ’，．．．，ＤａｔａＮＡ’からなるモジュールＤ３を書き込み回路１３に出力する。

また、情報分割回路１２は、情報Ｄａｔａ１Ｂ’，Ｄａｔａ２Ｂ’，Ｄａｔａ３Ｂ’，．．．，ＤａｔａＫＢ’，．．．，ＤａｔａＮＢ’からなるモジュールＤ４を書き込み回路１４に出力する。

【００２１】

書き込み回路１３は、情報分割回路１２から入力したモジュールＤ３を記録媒体１６に書き込む。

【００２２】

書き込み回路１４は、情報分割回路１２から入力したモジュールＤ４を記録媒体１７に書き込む。

【００２３】

以下、情報記録装置１の動作を説明する。

図３は、情報記録装置１の動作を説明するためのフローチャートである。

【００２４】

ステップＳＴ１１：

読み出し回路１０によって、記録媒体１５から図２に示す個人情報Ｄ１が読み出されて暗号化回路１１に出力される。

【００２５】

ステップＳＴ１２：

暗号化回路１１において、所定の暗号鍵を用いて、読み出し回路１０から入力された個人情報Ｄ１が暗号化されて図２に示す個人情報Ｄ２が生成され、当該個人情報Ｄ２が情報分割回路１２に出力される。

【００２６】

ステップＳＴ１３：

情報分割回路１２において、暗号化回路１１から入力された個人情報Ｄ２が、それぞれを単独では個人情報Ｄ１の秘匿性が保持される図２に示す２つのモジュールＤ３，Ｄ４に分割される。

そして、情報分割回路１２から書き込み回路１３にモジュールＤ３が出力され、情報分割回路１２から書き込み回路１４にモジュールＤ４が出力される。

【００２７】

ステップＳＴ１４：

書き込み回路１３によって、モジュールＤ３が記録媒体１６に書き込まれる。

書き込み回路１４によって、モジュールＤ４が記録媒体１７に書き込まれる。

【００２８】

以上説明したように、情報記録装置１によれば、図２に示すように、個人情報Ｄ１が、暗号化された後に、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ３，Ｄ４に分割され、モジュールＤ３，Ｄ４がそれぞれ物理的に独立した記録媒体１６，１７にそれぞれ記録される。

そのため、記録媒体１６，１７を別々に保管すれば、記録媒体１６，１７の一方が盗難され、しかも、盗難された記録媒体に記録されているモジュールの復号が盗難者によって行われた場合でも、個人情報Ｄ１の秘匿性は保たれる。

【００２９】

第２実施形態

図４は、本実施形態の情報復元装置３１の構成図である。

情報復元装置３１は、上述した第１実施形態の情報記録装置１によって、記録媒体１６と１７とに分割して記録された個人情報から、本来の個人情報Ｄ１を復元する。

図４に示すように、情報復元装置３１は、読み出し回路２０、，２１、情報合成回路２２、復号回路２３および書き込み回路２４を有する。

図４において、記録媒体１６および１７には、前述した第１実施形態で説明した図３に示す処理を経て、それぞれモジュールＤ３およびＤ４が記録されている。

【００３０】

読み出し回路２０は、記録媒体１６から読み出したモジュールＤ３を情報合成回路２２に出力する。

【００３１】

読み出し回路２１は、記録媒体１７から読み出したモジュールＤ４を情報合成回路２２に出力する。

【００３２】

情報合成回路２２は、図５に示すように、読み出し回路２０から入力したモジュールＤ３と、読み出し回路２１から入力したモジュールＤ４とを合成して個人情報Ｄ２を生成し、これを復号回路２３に出力する。

【００３３】

復号回路２３は、情報合成回路２２から入力した個人情報Ｄ２を、所定の復号鍵を用いて復号して個人情報Ｄ１を生成し、これを書き込み回路２４に出力する。

【００３４】

書き込み回路２４は、復号回路２３から入力した個人情報Ｄ１を、記録媒体１５に書き込む。

【００３５】

以下、情報復元装置３１の動作を説明する。

図６は、情報復元装置３１の動作を説明するためのフローチャートである。

【００３６】

ステップＳＴ２１：

読み出し回路２０によって、記録媒体１６から図５に示すモジュールＤ３が読み出されて情報合成回路２２に出力される。

また、読み出し回路２１によって、記録媒体１７から図５に示すモジュールＤ４が読み出されて情報合成回路２２に出力される。

【００３７】

ステップＳＴ２２：

情報合成回路２２において、図５に示すように、読み出し回路２０から入力したモジュールＤ３と、読み出し回路２１から入力したモジュールＤ４とが合成さ

れて個人情報Ｄ２が生成される。

個人情報Ｄ２は、情報合成回路２２から復号回路２３に出力される。

【００３８】

ステップＳＴ２３：

復号回路２３において、情報合成回路２２から入力した個人情報Ｄ２が、所定の復号鍵を用いて復号して個人情報Ｄ１を生成され、これが書き込み回路２４に出力される。

【００３９】

ステップＳＴ３４：

書き込み回路２４によって、復号回路２３から入力した個人情報Ｄ１が記録媒体１５に書き込まれる。

【００４０】

以上説明したように、情報復元装置３１によれば、正当な者が当該装置を用いることで、前述した第１実施形態の情報記録装置１によって別々の記録媒体１６，１７に格納されたモジュールＤ３，Ｄ４から個人情報Ｄ１を復元できる。

【００４１】

第３実施形態

図７は、本実施形態の情報記録装置４１の構成図である。

図７に示すように、情報記録装置４１は、読み出し回路５０、情報分割回路５１、暗号化回路５２，５３および書き込み回路５４，５５を有する。

情報記録装置４１は、記録媒体１５から読み出した個人情報Ｄ１を、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ１２，Ｄ１３に分割した後に暗号化してモジュールＤ１４，Ｄ１５を生成し、モジュールＤ１４を記録媒体１６に書き込み、モジュールＤ１５を記録媒体１７に書き込む。

【００４２】

読み出し回路５０は、記録媒体１５から読み出した個人情報Ｄ１を情報分割回路５１に出力する。

個人情報Ｄ１は、図８に示すように、情報Ｄａｔａ１～ＤａｔａＮからなる。

また、個人情報Ｄ１は、例えば、ユーザの個人ＩＤ情報や暗証番号、取り引き

の履歴情報、ユーザの名前、住所、経歴および職業などの秘匿性のある情報である。

【００４３】

情報分割回路５１は、読み出し回路５０から入力した個人情報Ｄ１を、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ１２，Ｄ１３に分割し、モジュールＤ１２を暗号化回路５２に出力し、モジュールＤ１３を暗号化回路５３に出力する。

図８に示すように、情報分割回路５１は、情報Ｄ１内の情報Ｄａｔａ１～ＤａｔａＮを、それぞれ情報Ｄａｔａ１ＡおよびＤａｔａ１Ｂ、情報Ｄａｔａ２ＡおよびＤａｔａ２Ｂ、情報Ｄａｔａ３ＡおよびＤａｔａ３Ｂ、．．．．、情報ＤａｔａＫＡおよびＤａｔａＫＢ、．．．．、情報ＤａｔａＮＡおよびＤａｔａＮＢに分割する。

そして、情報分割回路５１は、情報Ｄａｔａ１Ａ，Ｄａｔａ２Ａ，Ｄａｔａ３Ａ，．．．，ＤａｔａＫＡ，．．．，ＤａｔａＮＡからなるモジュールＤ１２を暗号化回路５２に出力する。

また、情報分割回路５１は、情報Ｄａｔａ１Ｂ，Ｄａｔａ２Ｂ，Ｄａｔａ３Ｂ，．．．，ＤａｔａＫＢ，．．．，ＤａｔａＮＢからなるモジュールＤ１３を暗号化回路５３に出力する。

【００４４】

暗号化回路５２は、所定の暗号鍵を用いて、情報分割回路５１から入力した個人情報Ｄ１２を暗号化して個人情報Ｄ１４を生成し、これを書き込み回路５４に出力する。

暗号化された個人情報Ｄ１４は、図８に示すように、それぞれ情報Ｄａｔａ１Ａ～ＤａｔａＮＡを暗号化した情報Ｄａｔａ１Ａ’～ＤａｔａＮＡ’からなる。

【００４５】

暗号化回路５３は、所定の暗号鍵を用いて、情報分割回路５１から入力した個人情報Ｄ１３を暗号化して個人情報Ｄ１５を生成し、これを書き込み回路５５に出力する。暗号化回路５３が用いる暗号鍵は、暗号化回路５２が用いる暗号鍵と同じものを用いてもよいし、異なるものを用いてもよい。

暗号化された個人情報Ｄ１５は、図８に示すように、それぞれ情報Ｄａｔａ１Ｂ～ＤａｔａＮＢを暗号化した情報Ｄａｔａ１Ｂ’～ＤａｔａＮＢ’からなる。

【００４６】

書き込み回路５４は、暗号化回路５２から入力したモジュールＤ１４を記録媒体１６に書き込む。

【００４７】

書き込み回路５５は、暗号化回路５３から入力したモジュールＤ１５を記録媒体１７に書き込む。

【００４８】

以下、情報記録装置１の動作を説明する。

図９は、情報記録装置４１の動作を説明するためのフローチャートである。

【００４９】

ステップＳＴ３１：

読み出し回路５０によって、記録媒体１５から図８に示す個人情報Ｄ１が読み出されて情報分割回路５１に出力される。

【００５０】

ステップＳＴ３２：

情報分割回路５１において、図８に示すように、読み出し回路５０から入力した個人情報Ｄ１が、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ１２，Ｄ１３に分割され、モジュールＤ１２が暗号化回路５２に出力され、モジュールＤ１３が暗号化回路５３に出力される。

【００５１】

ステップＳＴ３３：

暗号化回路５２において、図８に示すように、所定の暗号鍵を用いて、情報分割回路５１から入力した個人情報Ｄ１２が暗号化されて個人情報Ｄ１４が生成され、これが書き込み回路５４に出力される。

また、暗号化回路５３において、図８に示すように、所定の暗号鍵を用いて、情報分割回路５１から入力した個人情報Ｄ１３が暗号化されて個人情報Ｄ１５が生成され、これが書き込み回路５５に出力される。

【００５２】

ステップＳＴ３４：

書き込み回路５４によって、暗号化回路５２から入力したモジュールＤ１４が記録媒体１６に書き込まれる。

書き込み回路５５によって、暗号化回路５３から入力したモジュールＤ１５が記録媒体１７に書き込まれる。

【００５３】

以上説明したように、情報記録装置４１によれば、図８に示すように、個人情報Ｄ１が、それぞれを単独では個人情報Ｄ１の秘匿性が保持される２つのモジュールＤ１２，Ｄ１３に分割された後に暗号化されてモジュールＤ１４，Ｄ１５が生成され、モジュールＤ１４，Ｄ１５がそれぞれ物理的に独立した記録媒体１６，１７にそれぞれ記録される。

そのため、記録媒体１６，１７を別々に保管すれば、記録媒体１６，１７の一方が盗難され、しかも、盗難された記録媒体に記録されているモジュールの復号が盗難者によって行われた場合でも、個人情報Ｄ１の秘匿性は保たれる。

【００５４】

第４実施形態

図１０は、本実施形態の情報復元装置６１の構成図である。

情報復元装置６１は、上述した第３実施形態の情報記録装置４１によって、記録媒体１６と１７とに分割して記録された個人情報から、本来の個人情報Ｄ１を復元する。

図１０に示すように、情報復元装置６１は、読み出し回路７０，７１、復号回路７２，７３、情報合成回路７４および書き込み回路７５を有する。

図１０において、記録媒体１６および１７には、前述した第３実施形態で説明した図９に示す処理を経て、それぞれモジュールＤ１４およびＤ１５が記録されている。

【００５５】

読み出し回路７０は、記録媒体１６から読み出したモジュールＤ１４を復号回路７２に出力する。

【００５６】

読み出し回路７１は、記録媒体１７から読み出したモジュールＤ１５を復号回路７３に出力する。

【００５７】

復号回路７２は、読み出し回路７０から入力したモジュールＤ１４を、所定の復号鍵を用いて復号してモジュールＤ１２を生成し、これを情報合成回路７４に出力する。

【００５８】

復号回路７３は、読み出し回路７１から入力したモジュールＤ１５を、所定の復号鍵を用いて復号してモジュールＤ１３を生成し、これを情報合成回路７４に出力する。

【００５９】

情報合成回路７４は、図１１に示すように、復号回路７２から入力したモジュールＤ１２と、復号回路７３から入力したモジュールＤ１３とを合成して個人情報Ｄ１を生成し、これを書き込み回路７５に出力する。

【００６０】

書き込み回路７５は、情報合成回路７４から入力した個人情報Ｄ１を、記録媒体１５に書き込む。

【００６１】

以下、情報復元装置６１の動作を説明する。

図１２は、情報復元装置６１の動作を説明するためのフローチャートである。

ステップＳＴ４１：

読み出し回路７０によって、図１１に示すように、記録媒体１６からモジュールＤ１４が読み出されて復号回路７２に出力される。

また、読み出し回路７１によって、記録媒体１７からモジュールＤ１５が読み出されて復号回路７３に出力される。

【００６２】

ステップＳＴ４２：

復号回路７２において、読み出し回路７０から入力したモジュールＤ１４が、

所定の復号鍵を用いて復号されてモジュールＤ１２が生成され、これが情報合成回路７４に出力される。

また、復号回路７３において、読み出し回路７１から入力したモジュールＤ１５が、所定の復号鍵を用いて復号されてモジュールＤ１３が生成され、これが情報合成回路７４に出力される。

【００６３】

ステップＳＴ４３：

情報合成回路７４において、図１１に示すように、復号回路７２から入力したモジュールＤ１２と、復号回路７３から入力したモジュールＤ１３とが合成されて個人情報Ｄ１が生成され、これが書き込み回路７５に出力される。

【００６４】

ステップＳＴ４４：

書き込み回路７５によって、情報合成回路７４から入力された個人情報Ｄ１が、記録媒体１５に書き込まれる。

【００６５】

以上説明したように、情報復元装置３１によれば、正当な者が当該装置を用いることで、前述した第３実施形態の情報記録装置４１によって別々の記録媒体１６，１７に格納されたモジュールＤ１４，Ｄ１５から個人情報Ｄ１を復元できる。

【００６６】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、個人情報を分割して得た複数のモジュールを異なる記録媒体に記録する場合を例示したが、当該複数のモジュールを同じ記録媒体の異なる領域に記録してもよい。この場合に、記録媒体の何れの領域に何れもモジュールを記録したかを秘密にしておけば、当該記録媒体を不正に取得した者は、記録媒体から読み出したモジュールの合成の仕方が分からず、個人情報を復元できない。

【００６７】

また、上述した実施形態では、所定の情報を分割する前後の何れか一方で暗号

化を行う場合を例示したが、所定の情報を分割する前後の何れでも暗号化を行う場合、並びに所定の情報を分割する前後の双方で暗号化を行う場合でも本発明は適用可能である。

【００６８】

また、上述した実施形態では、本発明の所定の情報として、個人情報を例示したが、その他、映像、音声などの情報であってもよい。

【００６９】

また、上述した実施形態では、個人情報を２分割して２つの記録媒体１６，１７に記録する場合を例示したが、個人情報を３分割以上して３つ以上の記録媒体に記録してもよい。

【００７０】

【発明の効果】

以上説明したように、本発明によれば、情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録方法およびその装置と、そのような形態で情報が記録された記録媒体とを提供できる。

また、本発明によれば、上述したような情報記録方法およびその装置によって記録媒体に記録された情報を適切に復元できる情報復元方法およびその装置を提供できる。

【図面の簡単な説明】

【図１】

図１は、本発明の第１実施形態の情報記録装置の構成図である。

【図２】

図２は、図１に示す情報記録装置における処理の情報の流れを説明するための図である。

【図３】

図３は、図１に示す情報記録装置の処理のフローチャートである。

【図４】

図４は、本発明の第２実施形態の情報復元装置の構成図である。

【図５】

図５は、図４に示す情報復元装置における処理の情報の流れを説明するための図である。

【図６】

図６は、図４に示す情報復元装置の処理のフローチャートである。

【図７】

図７は、本発明の第３実施形態の情報記録装置の構成図である。

【図８】

図８は、図７に示す情報記録装置における処理の情報の流れを説明するための図である。

【図９】

図９は、図７に示す情報記録装置の処理のフローチャートである。

【図１０】

図１０は、本発明の第４実施形態の情報復元装置の構成図である。

【図１１】

図１１は、図１０に示す情報復元装置における処理の情報の流れを説明するための図である。

【図１２】

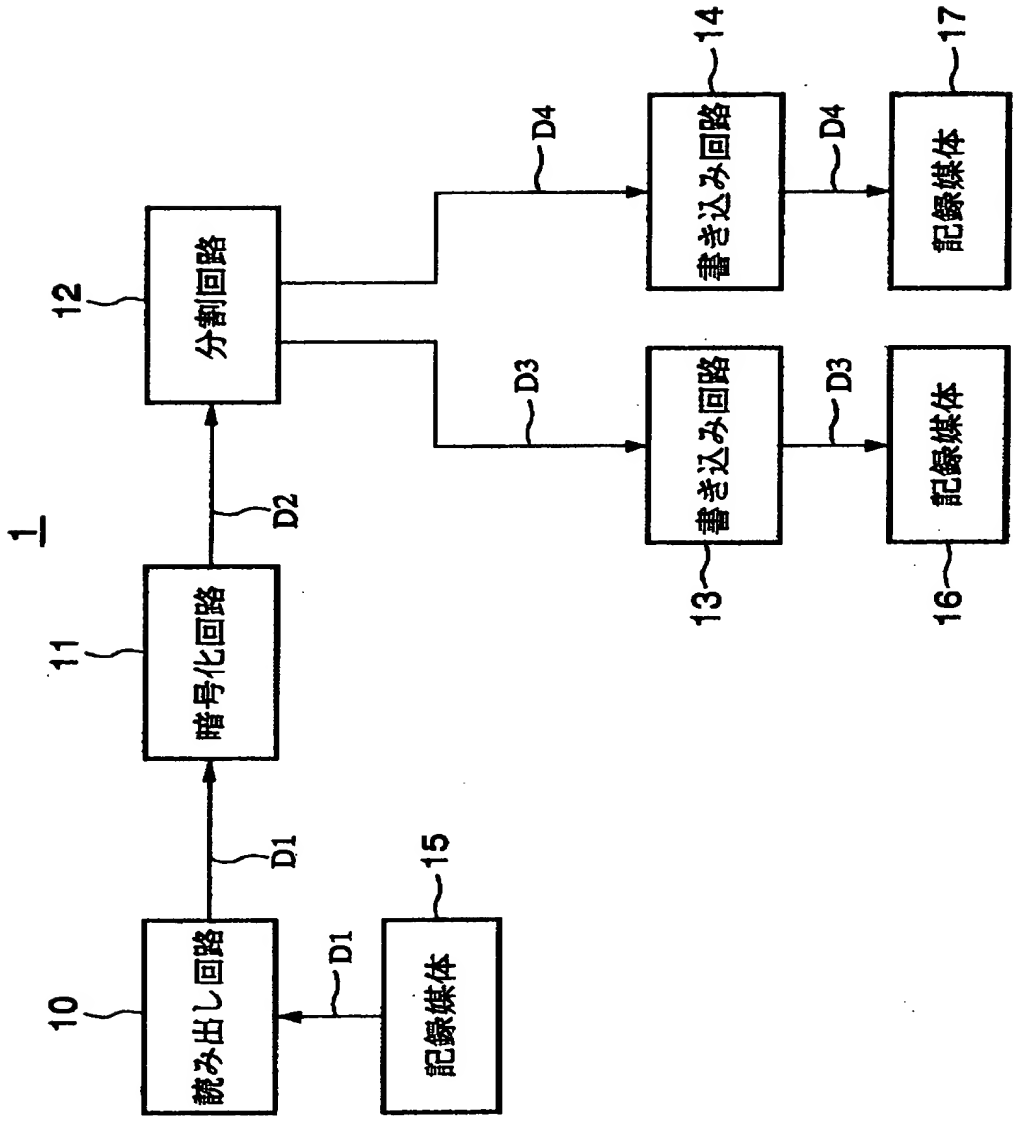
図１２は、図１０に示す情報復元装置の処理のフローチャートである。

【符号の説明】

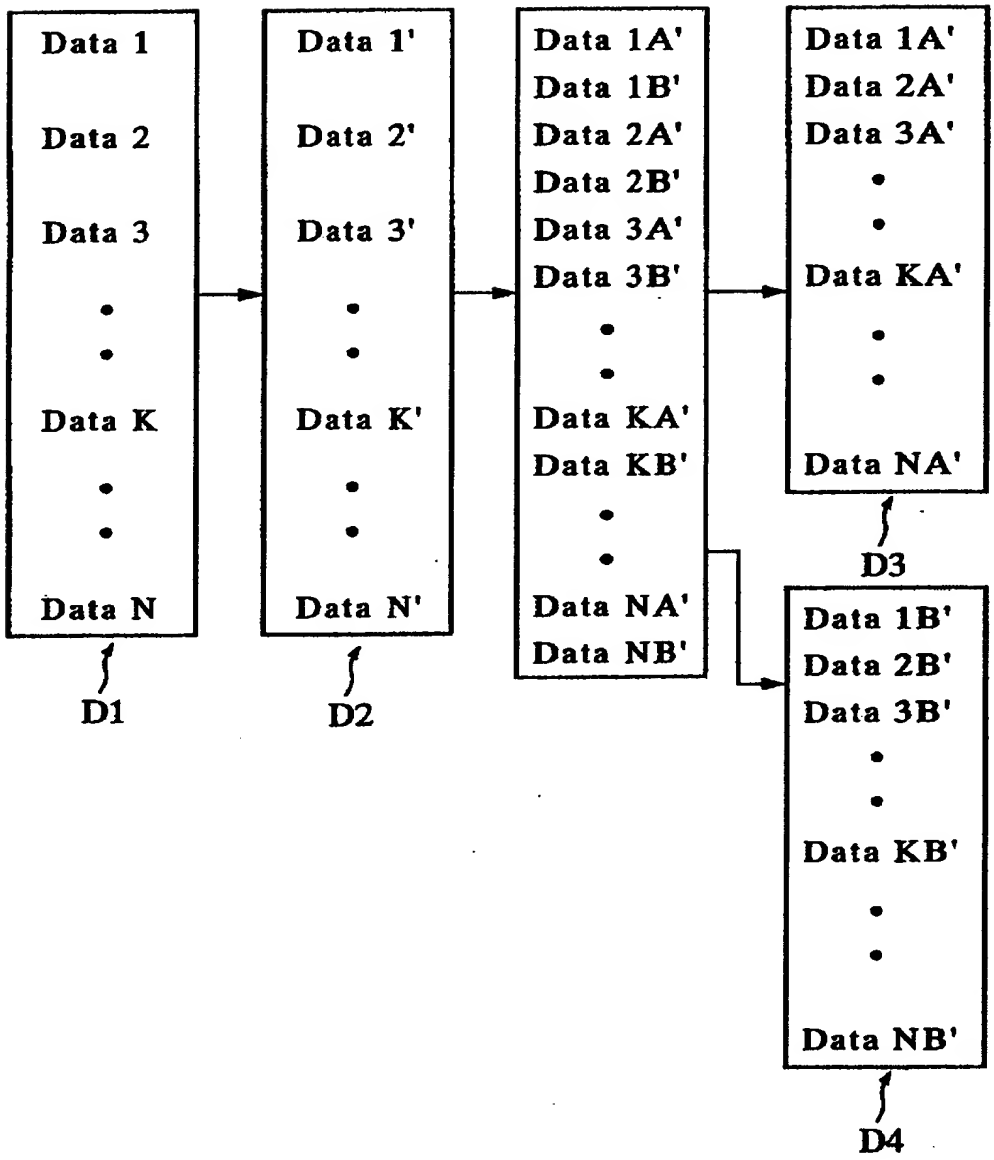
１…情報記録装置、１０…読み出し回路、１１…暗号化回路、１２…情報分割回路、１３，１４…書き込み回路、１５，１６，１７…記録媒体、２０，２１…読み出し回路、２２…情報合成回路、２３…復号回路、２４…書き込み回路、３１…情報復元装置、４１…情報記録装置、５０…読み出し回路、５１…情報分割回路、５２，５３…暗号化回路、５４，５５…書き込み回路、６１…情報復号装置、７０，７１…読み出し回路、７２，７３…復号回路、７４…情報合成回路、７５…書き込み回路

【書類名】　　図面

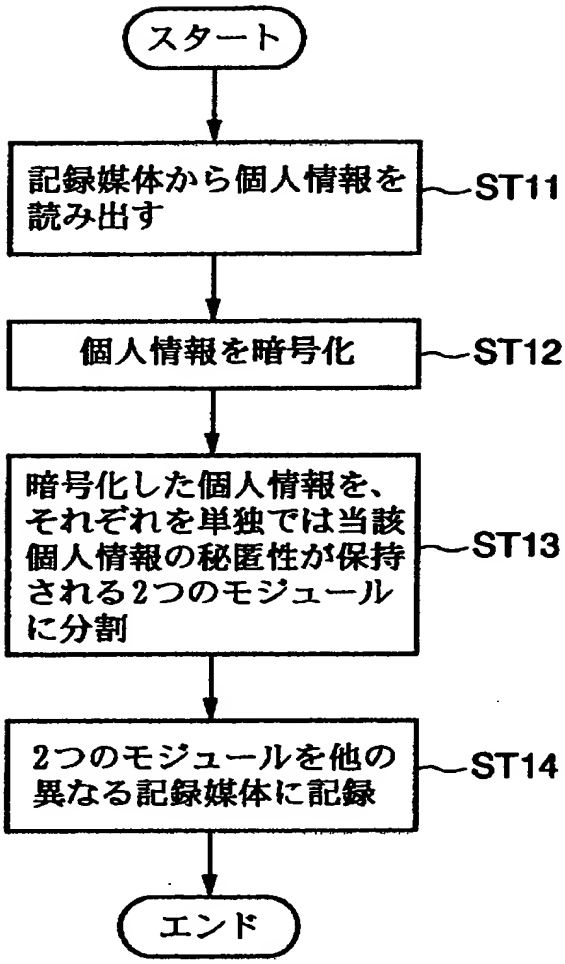
【図１】


1
10
読み出し回路
11
暗号化回路
12
分割回路
13
書き込み回路
14
書き込み回路
15
記録媒体
16
記録媒体
17
記録媒体
D1
D1
D2
D3
D3
D4
D4

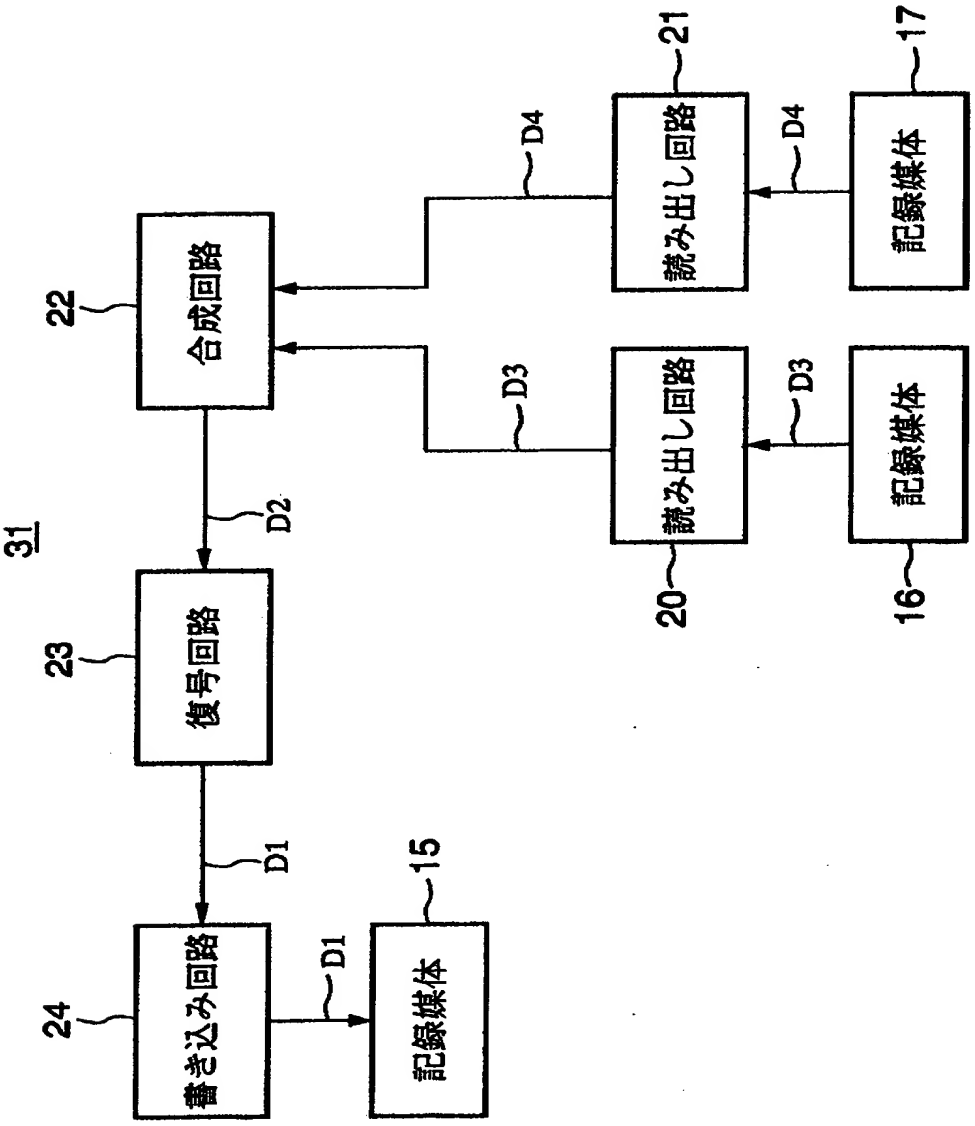
【図２】


Data 1
Data 2
Data 3
Data K
Data N
D1
Data 1'
Data 2'
Data 3'
Data K'
Data N'
D2
Data 1A'
Data 1B'
Data 2A'
Data 2B'
Data 3A'
Data 3B'
Data KA'
Data KB'
Data NA'
Data NB'
Data 1A'
Data 2A'
Data 3A'
Data KA'
Data NA'
D3
Data 1B'
Data 2B'
Data 3B'
Data KB'
Data NB'
D4

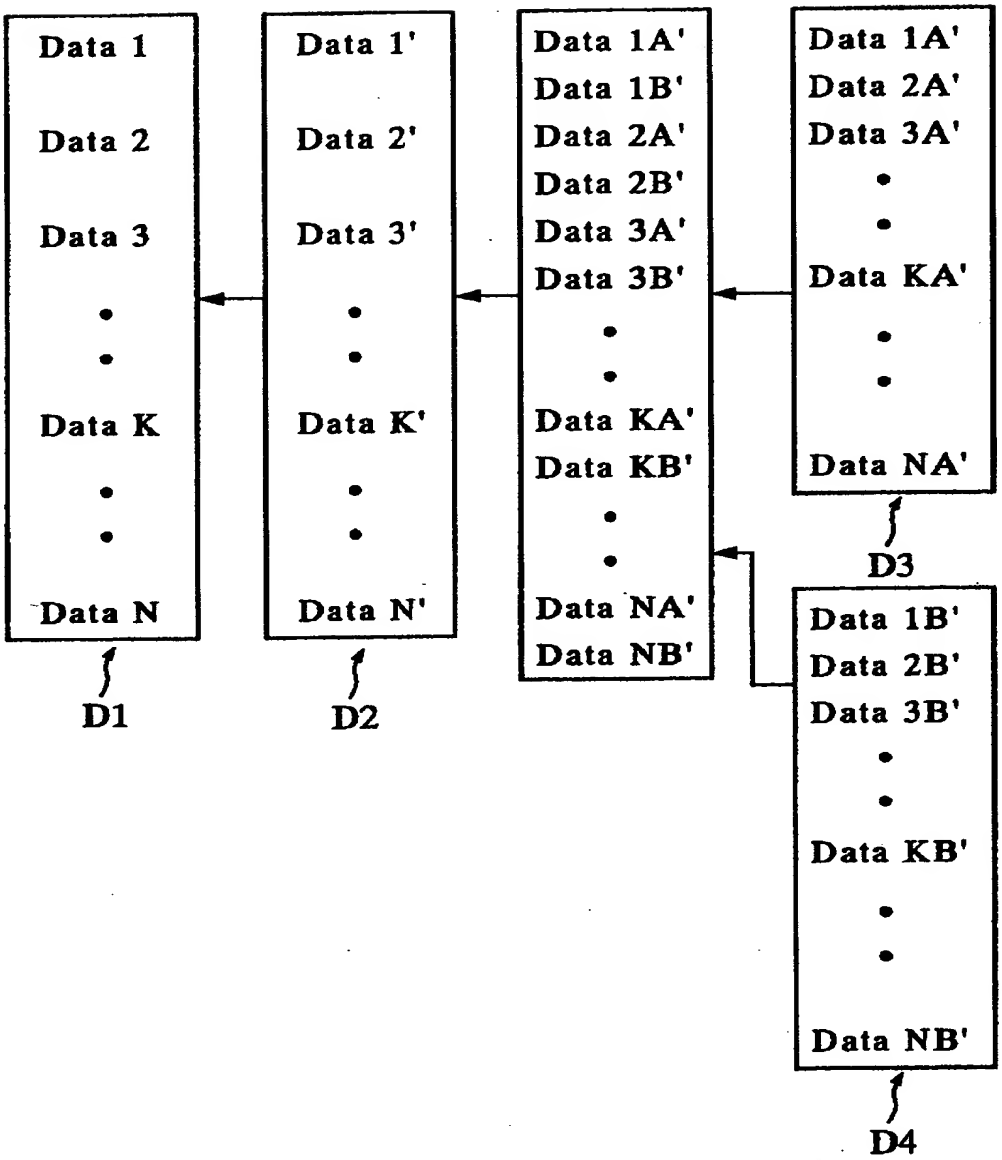
【図３】


スタート
記録媒体から個人情報を読み出す
ST11
個人情報を暗号化
ST12
暗号化した個人情報を、それぞれを単独では当該個人情報の秘匿性が保持される2つのモジュールに分割
ST13
2つのモジュールを他の異なる記録媒体に記録
ST14
エンド

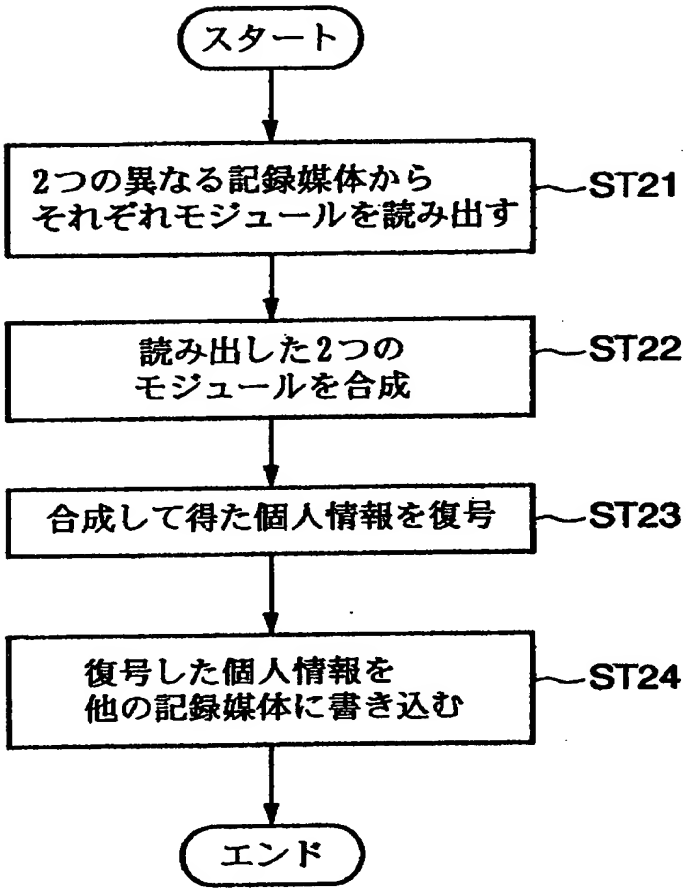
【図４】


31
22
合成回路
23
復号回路
24
書き込み回路
15
記録媒体
D1
D2
D3
D4
20
読み出し回路
21
読み出し回路
16
記録媒体
17
記録媒体

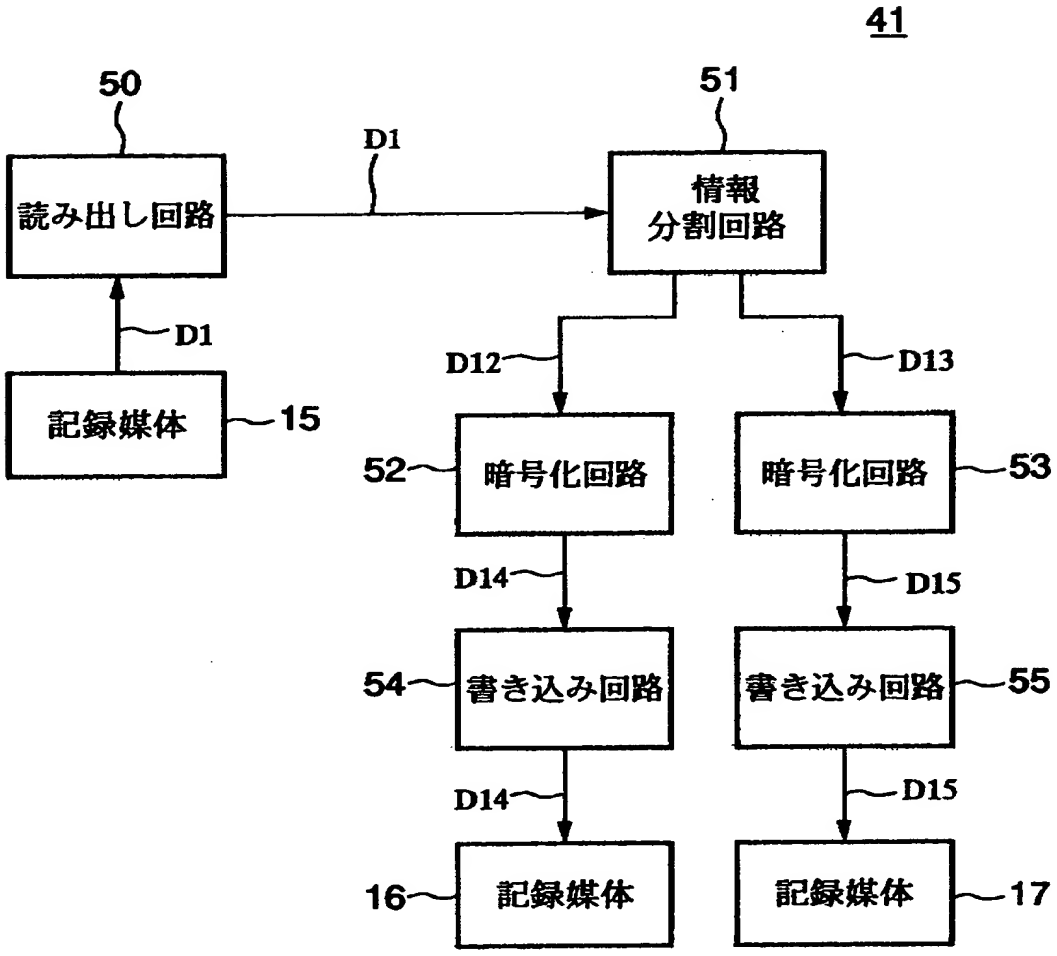
【図５】


Data 1
Data 2
Data 3
Data K
Data N
D1
Data 1'
Data 2'
Data 3'
Data K'
Data N'
D2
Data 1A'
Data 1B'
Data 2A'
Data 2B'
Data 3A'
Data 3B'
Data KA'
Data KB'
Data NA'
Data NB'
Data 1A'
Data 2A'
Data 3A'
Data KA'
Data NA'
D3
Data 1B'
Data 2B'
Data 3B'
Data KB'
Data NB'
D4

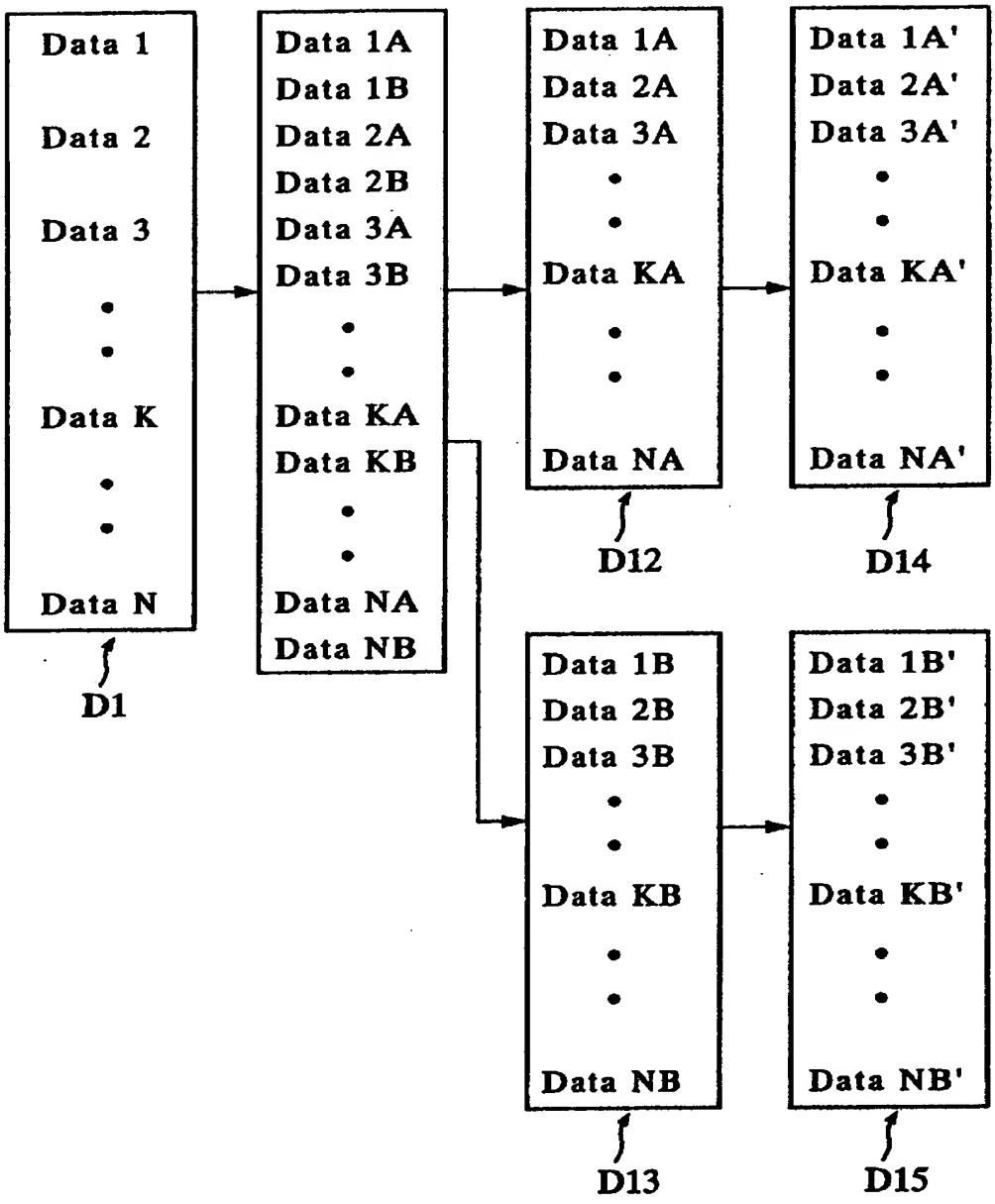
【図６】


スタート
2つの異なる記録媒体から
それぞれモジュールを読み出す
ST21
読み出した2つの
モジュールを合成
ST22
合成して得た個人情報を復号
ST23
復号した個人情報を
他の記録媒体に書き込む
ST24
エンド

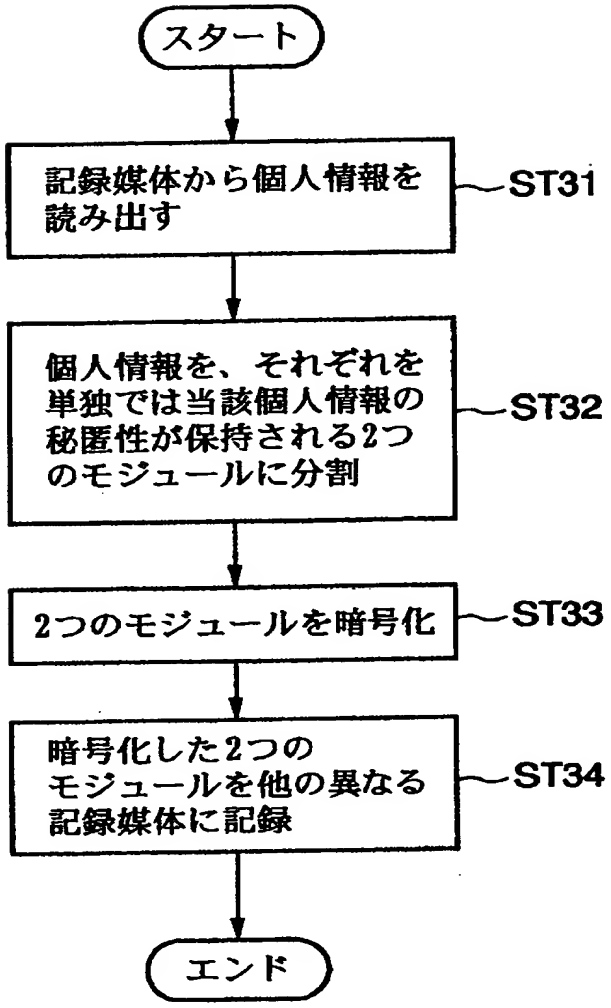
【図７】


41
50
51
D1
読み出し回路
情報
分割回路
D1
D12
D13
記録媒体
15
52
暗号化回路
暗号化回路
53
D14
D15
54
書き込み回路
書き込み回路
55
D14
D15
16
記録媒体
記録媒体
17

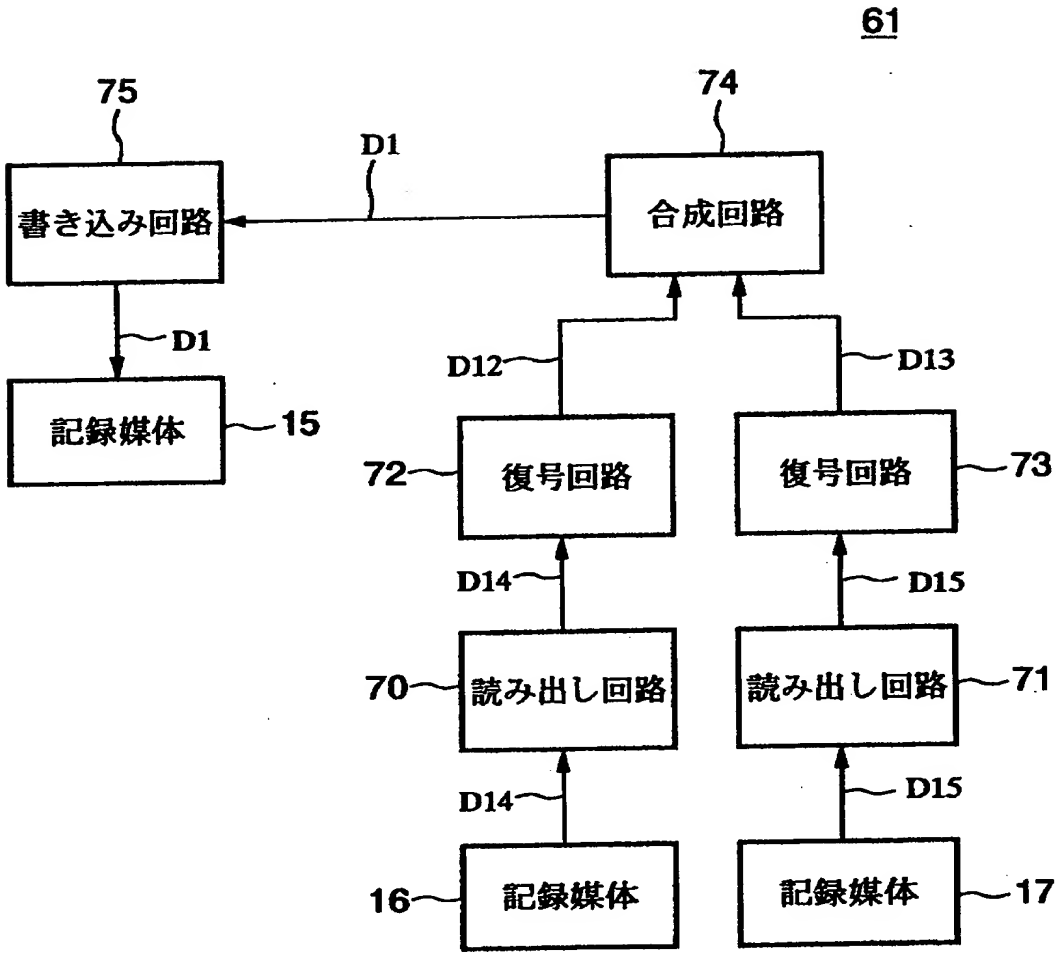
【図８】


Data 1
Data 2
Data 3
Data K
Data N
D1
Data 1A
Data 1B
Data 2A
Data 2B
Data 3A
Data 3B
Data KA
Data KB
Data NA
Data NB
Data 1A
Data 2A
Data 3A
Data KA
Data NA
D12
Data 1A'
Data 2A'
Data 3A'
Data KA'
Data NA'
D14
Data 1B
Data 2B
Data 3B
Data KB
Data NB
D13
Data 1B'
Data 2B'
Data 3B'
Data KB'
Data NB'
D15

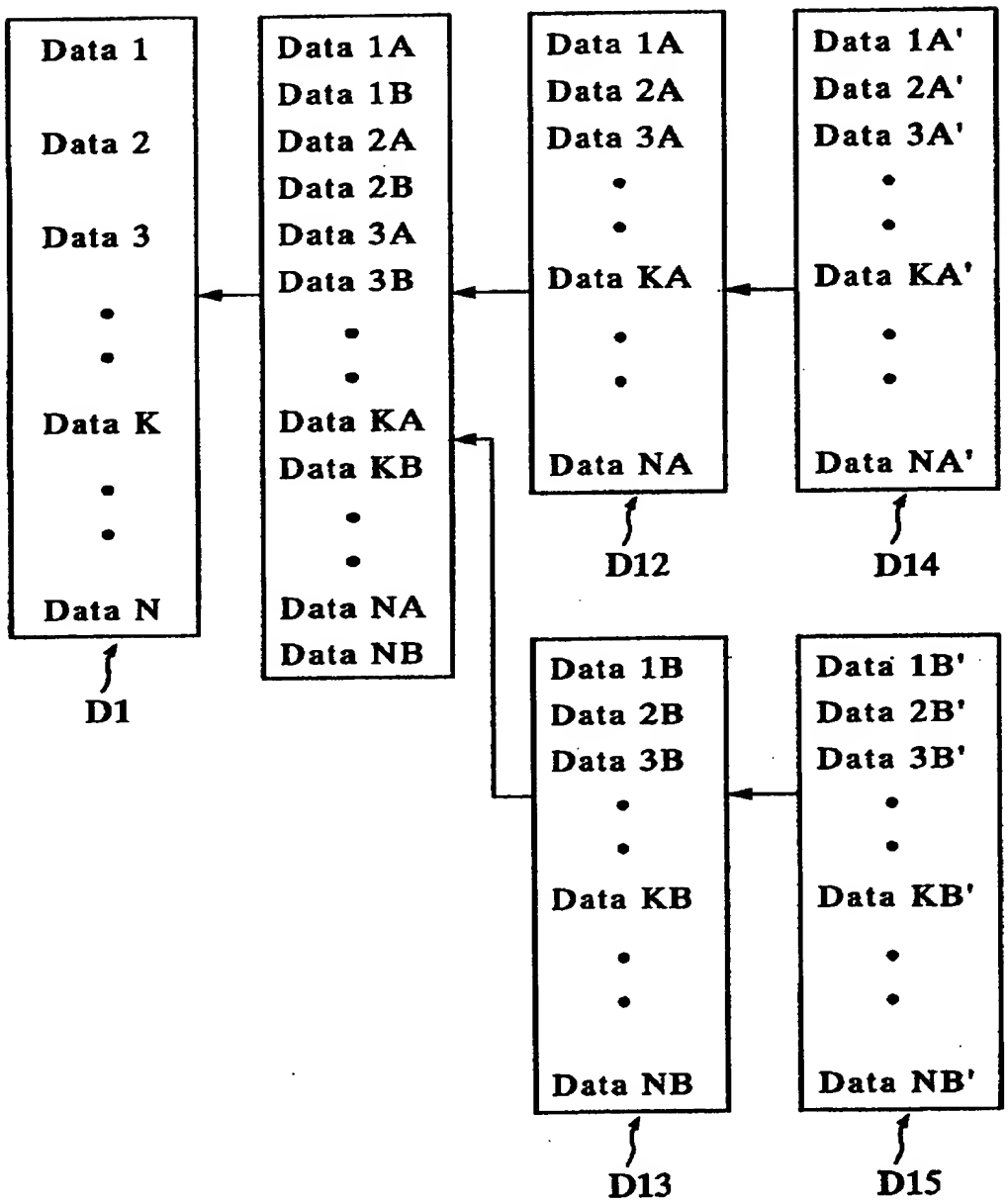
【図９】


スタート
記録媒体から個人情報を読み出す
ST31
個人情報を、それぞれを単独では当該個人情報の秘匿性が保持される2つのモジュールに分割
ST32
2つのモジュールを暗号化
ST33
暗号化した2つのモジュールを他の異なる記録媒体に記録
ST34
エンド

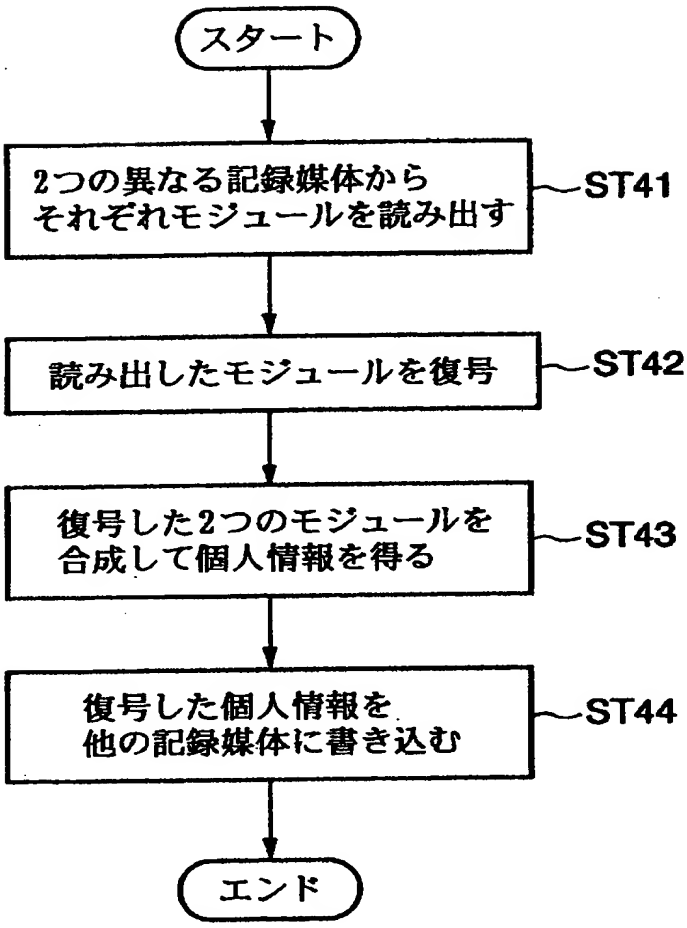
【図１０】


61
75
74
D1
書き込み回路
合成回路
D1
D12
D13
記録媒体
15
72
復号回路
復号回路
73
D14
D15
70
読み出し回路
読み出し回路
71
D14
D15
16
記録媒体
記録媒体
17

【図１１】


Data 1
Data 2
Data 3
Data K
Data N
D1
Data 1A
Data 1B
Data 2A
Data 2B
Data 3A
Data 3B
Data KA
Data KB
Data NA
Data NB
Data 1A
Data 2A
Data 3A
Data KA
Data NA
D12
Data 1A'
Data 2A'
Data 3A'
Data KA'
Data NA'
D14
Data 1B
Data 2B
Data 3B
Data KB
Data NB
D13
Data 1B'
Data 2B'
Data 3B'
Data KB'
Data NB'
D15

【図１２】


スタート
2つの異なる記録媒体から
それぞれモジュールを読み出す
ST41
読み出したモジュールを復号
ST42
復号した2つのモジュールを
合成して個人情報を得る
ST43
復号した個人情報を
他の記録媒体に書き込む
ST44
エンド

【書類名】　　要約書

【要約】

【課題】　情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録装置を提供する。

【解決手段】　記録媒体１５から読み出し回路１０によって読み出した個人情報を、情報分割回路１２において、それぞれ単独では当該個人情報の秘匿性が保持される２つのモジュールＤ３，Ｄ４に分割する。書き込み回路１３によって、モジュールＤ３を記録媒体１６に書き込み、書き込み回路１４によってモジュールＤ４を記録媒体１７に書き込む。

【選択図】　図１

出願人履歴情報

識別番号　〔０００００２１８５〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社